REMARKS

As further evidence of the non-obviousness of the claimed invention, the applicants submit herewith a number of publications written either by the applicants or others who have come to recognize the importance of trade secret protection. The articles include:

"The Economic Valuation of Trade Secret Assets", R. Mark Halligan and Richard F. Weyand, Journal of Internet Law, February 2006

"The NSA's Interception of Emails and Phone Calls in the US is Unlawful", Randy Gainer, Journal of Internet Law, February 2006

"Duty to Identify, Protect Trade Secrets Has Arisen", R. Mark Halligan, The National Law Journal, August 19, 2005

"Accounting for Trade Secret Assets", R. Mark Halligan and Richard F. Weyand, Executive Counsel, March/April 2006

"The Sorry State of Trade Secret Protection", R. Mark Halligan and Richard F. Weyand, The Corporate Counsellor, Law Journal Newsletters, August 2001

"Trade Secret Holding Companies: A Structural Solution to a Sarbanes-Oxley Requirement", R. Mark Halligan and Richard F. Weyand, IP Law 360, Portfolio Media 2006

"Keep Your Chief Assets Secret", John Yuva, Inside Supply Management, April 2006

"Complying with SOX in the Information Age", John Yuva, Inside Supply Management, May 2006

Allowance of claims 1-52, as now presented, is believed to be in order and such action is earnestly solicited. Should the Examiner be of the opinion that a telephone conference would expedite prosecution of the subject application, he is respectfully requested to telephone applicant's undersigned attorney.

Respectfully submitted,
WELSH & KATZ, LTD.

By
Jon P. Christensen
Registration No. 34,137

June 7, 2006
WELSH & KATZ, LTD.
120 South Riverside Plaza
22nd Floor
Chicago, Illinois 60606
(312) 655-1500

The Economic Valuation of Trade Secret Assets

By R. Mark Halligan and Richard F. Weyand

The economic valuation of trade secret assets has perplexed the intellectual property bar for years. The economic and legal issues are seemingly inextricably intertwined. We present here a method for valuation of trade secret assets that decouples the economic and legal issues, rendering the problem tractable.

Several accepted methods exist for the valuation of a property. Depreciated cost, replacement cost, fair market value, and net present value of future cash flows are all proper measures in specific circumstances.

For intellectual property, however, depreciated cost is not appropriate. The direct acquisition cost of intellectual property may be insignificant, as when the intellectual property results from a flash of insight. However, that same insight may result from the sudden emergence of an idea after years of study in the field and years of experimentation in the laboratory. Which, then, is the true cost, the negligible cost of a moment's insight or the sum total cost of the education and experience of a lifetime?

Similarly, replacement cost is problematic. How does one replace a flash of insight? By what means can one predict the machinery of invention? For patents, trademarks, and copyrights, injunctive relief is true replacement, that is, the restoration of the exclusive use of the intellectual property. But trade secrets, once lost in the public domain, are lost forever. The bell cannot be unrung. How then can a replacement cost even be conceptualized, much less determined?

As for fair market value, there may be no marketplace for the intellectual property in question. An advance in the method of manufacturing a proprietary product, a unique corporate organizational structure or compensation plan, negative know-how, that is, knowledge about what doesn't work—none of these intellectual properties has a marketplace from which a fair market value may be obtained.

What we are left with, then, for trade secrets is the ***net present value of future cash flows***. This is a particularly appropriate measure for trade secrets because the very essence of a trade secret anticipates future cash flows. A trade secret is any information not generally known in the trade, which the owner has made appropriate efforts to keep secret and which confers a ***competitive advantage*** from being kept secret. The net present value of future cash flows resulting from that competitive advantage is an appropriate method for placing a dollar amount on the current value of a trade secret asset.

THE NET PRESENT VALUE OF FUTURE CASH FLOWS METHOD

Net present value of a future cash flow requires an evaluation of three factors:

1. The total amount of future cash flow,
2. The discounted basis of that future cash flow as a present value, and
3. The probability of the future cash flow occurring.

If values can be assigned to these three factors, then the economic value of a trade secret can be calculated by multiplying these three factors together.

The total amount of the future cash flow is the total amount of income over time that will be derived from keeping the information secret as compared to the expected income over time if the information was in the public domain. This is analogous to the valuation of patents, where the economic value of the patent is the value of the exclusive use of the invention as compared to the situation in which the invention is available for use by all.

It may be legitimately asked whether there isn't a broader altruistic value in discovering new knowledge for the use of all, to the benefit of everyone. There is such value, but it is not economic value, that is, it is not a value on which a price can be put, such as in the sale or license of a technology. No one will pay for the use of public domain knowledge, and so the fair market value of such knowledge is zero.

Note that there may be more than one legitimate possessor of a trade secret in the marketplace. Calculation of the net present value of trade secrets is much easier if the trade secret is an invention not known at all in the trade. Since in practice it is impossible to determine whether one's competitors already have legitimate possession of the same information and are also holding it as a trade secret, the simple calculation of value comparing the situations of exclusive possession to public domain exposure is appropriate.

R. Mark Halligan is a principal at Welsh & Katz, Ltd. Richard F. Weyand is president of The Trade Secret Office, Inc.

Misappropriation creates another possessor of the trade secret without the trade secret owner's authorization or consent. Under these circumstances, the damages evaluation compares the pre-misappropriation market to the post-misappropriation market, and the plaintiff can obtain its lost profits and disgorgement of the misappropriator's ill-gotten gains to the extent not already taken into consideration in calculating the trade secret owner's losses. If other competitors remain ignorant of the information, the damages so calculated will be some portion of the total value calculated when comparing the situations of exclusive possession to public domain exposure.

The second factor in the trade secret valuation model, the discounted basis of a future cash flow, is that percentage of the future cash flow that must be invested now as principal to realize the calculated future cash flows over the expected life cycle of the trade secret. This is a traditional accounting method for the calculation of the present value of a future income stream.

The last factor in the trade secret valuation model is the probability of future cash flows derived from the trade secret asset, which can be calculated by evaluating and determining the probability of prevailing in a civil lawsuit to defend the trade secret asset. This has been the critical barrier preventing the economic valuation of trade secret assets because it has been widely held that the probability of prevailing in a future litigation cannot be calculated. The authors disagree with this general consensus.

A trade secret can be validated only in litigation. Until there is a judgment entered in a civil lawsuit that the plaintiff possesses a trade secret, there is no legal trade secret status. In contrast, there is a presumption of validity when patent, copyright, and trademark certificates are issued by the United States government. An official certificate defines the specific intellectual property right that exists.

TRADE SECRETS IN LITIGATION

Trade secrets, however, remain inchoate and subject to the vagaries of the litigation process. The burden of proof is on the trade secret owner to show the existence of a trade secret as plaintiff in a misappropriation lawsuit. The plaintiff cannot rely on presumptions flowing from a prior *ex parte* examination by the federal government.

There are four proofs required to prevail on an assertion of trade secret protected status in court:

1. Existence. The information must qualify as a trade secret asset.
2. Ownership. The plaintiff must be able to prove ownership of the information.
3. Access. The plaintiff must prove the defendant had access to the information, that is, that the defendant did not independently re-invent the trade secret.
4. Notice. There must be actual, implied or constructive notice of the trade secret status of the information prior to the misappropriation.

Failure of any of these four essential proofs puts the trade secret assets at risk.

The identification of the *res* is critical to proving existence in trade secret litigation. What is "it" that is alleged to be a trade secret? Any information, technical or non-technical, can qualify under the modern definition of a trade secret if the information is not generally known in the trade, there have been appropriate steps taken to protect the secrecy of the information, and there is an actual competitive advantage derived from the secrecy of the information.

These inquiries inevitably require a careful consideration of the following six factors derived from the original definition of a trade secret in the United States in § 757 of the First Restatement of Torts:

1. The extent to which the information is known by outsiders;
2. The extent to which the information is known by insiders;
3. The measures taken to guard the secrecy of the information;
4. The value of the information to the information owner's current operations and the value if obtained by competitors;
5. The amount of time, effort, and money expended to obtain the information; and
6. The ease or difficulty of reverse engineering the information.

All six factors need not be present. However, the six factors will be considered by the trier of fact, and the probability of the existence or non-existence of a trade secret can only be determined after all the six factors have been evaluated and considered.[1]

In litigation, the defendant will dispute all six factors and further argue (1) that the information is generally known in the trade, (2) that it was not reasonably protected, and (3) that it confers no competitive advantage. Plaintiff need not prevail on all six factors, but the plaintiff ***must prevail*** on the three essential elements of the modern definition of a trade secret outlined earlier. Failure of proof on any one of these essential elements will invalidate the existence of a trade secret.

With regard to the first prong of the modern definition, not generally known in the trade, experience in trade secret misappropriation cases has shown that an "everyone knows it" defense does not prevail absent evidentiary substantiation. The defendant must come forward with

evidence from industry publications or present evidence from persons skilled in the art to convince the trier of fact that the information is generally known and used by the other competitors in the marketplace.

The second prong of the modern definition causes the most trouble in real situations. What are appropriate measures to protect the trade secret? The test is defined as relative secrecy, not absolute secrecy. Measures approaching absolute secrecy would prevent exploitation of the trade secret to obtain the resulting economic advantage. Relative secrecy means taking reasonable measures under the circumstances. For example, if a company has already suffered a computer theft of trade secrets, the courts expect a higher level of security in the face of this established and known threat. Courts also apply a sliding-scale analysis to corporations based on size. Larger corporations are expected to have more sophisticated trade secret protection measures than a mom-and-pop business.

The burden of establishing reasonable security measures rests upon the plaintiff. Security measures help the courts define what "it" is that is being protected as a trade secret. For example, if a lockbox is the security measure, then the contents of the lockbox must be the trade secrets. Second, reasonable security measures establish the property interests in the trade secret. Stated differently, why should the courts protect the alleged trade secret if the plaintiff has failed to protect it? The standard of care in the industry comes into play with respect to this prong. Courts will look to the security measures of other competitors in the industry to determine whether the plaintiff has executed the requisite amount of reasonable care

Finally, the third prong of the definition requires competitive advantage, that is to say, an economic advantage. This advantage can take the form of increased revenues or profits for the owner of the information, but it can also take the form of a reduced ability of other firms to compete effectively against the owner of the information. That is, either the trade secret owner's competitive position is enhanced by the possession of the information or the competitors' position is diminished by lack of knowledge of the information. Trade secrets also deter entry of new market entrants who must spend the time, effort, and money, go down all the blind alleys, and engage in all the trial and error necessary to compete against the existing competitors in the market.

The second required proof, ownership, has been implied but has not often been litigated, probably because the word "ownership" is not expressly included in the definition. However, it is critical that the possessor of a trade secret have ownership or be a licensee of the owner. The intellectual property laws in the United States protect the creator with few exceptions (*e.g.*, the work-for-hire doctrine in the copyright statute), and the plaintiff must show ownership of the trade secret. Absent an employee-assignment clause in a valid and enforceable employment contract, the result in litigation may be that a trade secret does in fact exist, but it was created and is owned by the employee. The company may retain no more than a shop right to practice the inventions embodied in the trade secret because it was created with company tools on company time

Access is an important proof to secure the plaintiff's trade secret rights. There is no monopoly right in trade secrets. If the defendant can show that the trade secret was independently developed without access or use of the plaintiff's information, then the defendant has the right to practice the inventions or improvements embodied in the trade secret. Trade secret protection can be extended only to prevent actions by employees or third parties that obtain access to the information in confidence and breach that obligation of confidentiality.

Finally, notice of the trade secret status of the information is necessary. The courts will imply constructive notice in a principal-agency relationship under certain circumstances. With respect to third parties, however, failure to provide notice and to obtain an agreement to maintain the information as confidential ***before*** actual disclosure may result in forfeiture and therefore be fatal to the trade secret claim. This is why nondisclosure agreements (NDAs) and confidential disclosure agreements (CDAs) must be executed before third-party disclosures. Although a writing is not required to establish notice, it is clearly preferred to the conflicting testimony of witnesses in a subsequent court hearing.

Notice can take the form of "confidential and proprietary" labels on sensitive documents, a high-level description of the trade secrets on a trade secret exit interview form, or password-protected access on a computer. The failure to mark a document as confidential is not fatal, however, if it can be independently established that the recipient knew or had reason to know that the information was confidential and that the recipient was not authorized to take and use the information for his own benefit or the benefit of others without the trade secret owner's consent.

It is important to note that this required notice cannot take the lackadaisical form that "everything we do is a trade secret." A failure to differentiate the trade secret information from the public domain information within the company places all information in the same class. Companies have found that, when they claim that "everything" is a trade secret, the courts conclude that "nothing" is a trade secret. There is no substitute for the

specific identification and protection of trade secret assets by a company.

Where does all this leave us with regard to the economic valuation of a trade secret? There are two important observations to make at this point.

First, the **total value** of all the potential trade secret information of a company that has failed to meet the evidentiary criteria outlined above should be set at ***exactly zero***. There is no inherent right to obtain trade secret status in information absent proper stewardship, and, absent such stewardship, the probability of prevailing on the merits in future litigation alleging trade secret status for the information approaches zero.

Second, the valuation of a trade secret is not confined to the value of the information content *per se*. ***The valuation of a trade secret asset is a function of both the content of the trade secret information and the stewardship and protection of the trade secret asset.***

This fundamental principle of trade secret asset valuation presents good news and bad news scenarios to corporations faced with the task of performing an economic valuation of their trade secret assets.

It is certainly bad news to the well-meaning but poorly prepared client, after the misappropriation, on the brink of litigation, that its suit has little chance of success due to poor stewardship. The good news is that the implementation of procedures for the proper stewardship and protection of trade secrets ***before misappropriation*** can both ensure and increase the economic value of those assets.

CASE STUDY

We present the following case study to illustrate these principles. As trade secret cases are by definition very sensitive, this case study is necessarily hypothetical. We have combined certain common issues that we have seen in actual cases in order to construct a likely scenario.

In our example, the owner of a closely held company has contacted you to perform an economic valuation of its trade secret portfolio. You perform an initial investigation and find that:

1. There is no inventory of the alleged trade secrets.
2. There are no employee agreements beyond the statutory fiduciary obligations.
3. There are no contractor or visitor agreements.
4. Alleged trade secret information is not secured in locked file cabinets, and such information is often left out in the open on company desks in unlocked offices.
5. Alleged trade secret information is stored on personal computers on which login protections have not been implemented.
6. Documents containing potential trade secrets are not stamped or labeled confidential or proprietary.
7. There is no secure method for destroying confidential documents.
8. No method is in place to track the time, effort, and money expended in creating and developing the alleged trade secret information.
9. Employee, contractor, and visitor badges are not required.
10. There is no security at the front door.
11. The manufacturing processes are not hidden from public view.
12. Temporary workers are often hired during peak periods and exposed to the alleged trade secrets.
13. There is no policy handbook on trade secrets, and no training in trade secret handling procedures for employees.
14. There are no trade secret exit interviews of departing employees.

You inform the business owner that the valuation of his trade secrets has been performed, at far less expense than he had hoped. That's the good news. The bad news is that the economic value of his trade secret information is exactly zero. While the content may or may not have economic value from not being generally known in the trade, there is little probability that the company can or will prevail in litigation. Why should the courts protect information that the company itself has not protected? The company risks forfeiture of its trade secret rights to anyone exposed to such information who can then legally appropriate them for his or her own benefit.

The owner of the company is appalled by the results of your valuation study, shared in confidence with the client. How can this information, developed over many years at great expense, have an economic value of zero? The answer is clear. There is no inherent right or title to trade secrets absent proper stewardship. There is undoubtedly information that provides an economic advantage, but the company has voluntarily exposed it to the world without restriction, and any trade secret rights in this information are at immediate risk of forfeiture.

The case law is replete with examples of this hypothetical. Many information owners find out when it is too late that the courts will not protect their information assets as trade secrets because the company has taken inadequate measures to protect such information, or a forfeiture of any trade secret rights in such information has occurred. Information is either a trade secret or not a trade secret. Absent a patent, if the information is not a trade

secret, then the information can be legally appropriated and used by others for their own benefit or the benefit of others.

The unfortunate result in *Omega* v. *Chroma*[2] is illustrative. Several former Omega employees formed a new company using Omega proprietary technology. Omega sued the defendants for trade secret misappropriation. The trial court found that the information at issue was protectible as a trade secret, but Omega lost because the court found that Omega had failed to take reasonable steps to protect the information. Omega's appeal to the Vermont Supreme Court centered on the trial court's finding that the substantial amounts of information acquired and used by the former employees were found to qualify as "trade secrets" by the trial court thereby entitling Omega to judgment as a matter of law. However, the Vermont Supreme Court rejected this argument and affirmed the trial court. The failure of Omega to take adequate steps to protect its trade secret assets resulted in a forfeiture of these trade secret assets and a finding that the former Omega employees owed no duty of confidentiality to Omega.

PROTECTING BEFORE MISAPPROPRIATION

However, in many circumstances, it is *not* too late to change the economic value of the assets because there has been no misappropriation yet. To protect the economic value of trade secret assets, the following basic steps must be implemented.

- An inventory of the potential trade secret assets should be conducted immediately. In practical terms, this will involve the preparation of a list of trade secrets with documentation of the dates of creation, places of storage, places of use, and other key information necessary for the maintenance of these assets on an on-going basis.
- Employee, contractor, and visitor agreements should be implemented. Careful attention should be paid to both confidentiality and ownership issues, with contractual assignment clauses being implemented where necessary.
- With respect to paper documents and tangible items, procedures for locked file cabinets or other security measures should be implemented.
- Electronic security procedures should be implemented, including, at a minimum, the implementation of login protections on personal computers.
- Access to information should be on a need-to-know basis. Sign-out/sign-in procedures should be used. Confidential documents should be marked "confidential." Super-confidential documents should be marked "super-confidential," and access should be severely restricted.
- Locked bins should be used to discard confidential documents, and an outside company performing onsite document destruction should maintain the bins.
- Accounting procedures should be implemented to track the time, effort, and money expended on the creation and development of trade secret assets.
- All persons should wear prominently displayed badges while on the premises. A visitor sign-in/sign-out badge system should be implemented.
- Manufacturing processes should be restricted from public view.
- The company handbook should devote an entire section to trade secrets. There should be ongoing employee education on the importance of identifying and documenting the existence of trade secret assets, with employee economic incentives for complying with this policy.
- The company should implement a strict procedure for trade secret exit interviews.

Once the information is secure and ownership, access, and notice issues are under control, we have changed the zero probability of being able to defend the trade secret information and its resulting future cash flows to a near certainty that protected status will be granted. At this point, the evaluation of the economic value of the ***content*** of the trade secret information can be performed in the same manner as currently practiced for patents. Finally, the current economic value of the trade secret information can be calculated by multiplying the three factors described earlier.

MANAGING TRADE SECRETS

We conclude with a short discussion of an important further distinction between trade secrets and the other intellectual properties—patents, copyrights, and trademarks—and the implications of this distinction. The actual number of patents, copyrights, and trademarks owned by most companies is small, numerable, and changes slowly over time.

In contrast, even small companies may have a very large number of trade secrets. These trade secrets are not so well bounded and defined as patents, copyrights, and trademarks, and so they tend to blend into each other, forming an interlocking mesh of information that does not easily divide into separate, countable, and distinct trade secrets. Finally, trade secrets are created and destroyed rapidly in an information economy, making the management of trade secrets a dynamic process.

The dynamic trade secret environment of firms in our modern economy has led many to conclude that it is simply too difficult, even overwhelming, to address all of these rapidly changing assets on any organized basis. However, the marketplace is demanding an accounting system to track and value intangible information assets. We therefore must provide appropriate solutions for the management of trade secrets by our clients.

The computer revolution that is driving the dynamic trade secret environment holds the promise of a solution as well. Automated systems for the inventorying, tracking, and life-cycle management of trade secrets are becoming available, and we must incorporate these solutions in providing quality intellectual property legal services. As these systems come into wider use, the relative standard of appropriate care for trade secret information will come to include such systems as a necessary element of proper stewardship.

NOTES

1. *See* Learning Curve Toys, Inc. v. Playwood Toys, Inc., 342 F.2d. 714 (7th Cir. 2003).
2. Omega v. Chroma, 174 Vt. 10, 800 A.2d 1064 (2002).

JOURNAL OF INTERNET LAW
Distribution Center
7201 McKinney Circle
Frederick, MD 21704
www.aspenpublishers.com

9900502555

LAW JOURNAL NEWSLETTERS

The Corporate Counsellor

Volume 16, Number 3

August 2001

PROPRIETARY RIGHTS

The Sorry State Of Trade Secret Protection

By R. Mark Halligan and Richard F. Weyand

It's your worst nightmare. Your company's major asset is completely unprotected. Careless or untrained employees are giving it away. Disgruntled ex-employees are stealing it outright. Your competitors are actively engaged in professional and well-directed efforts to take it. It is poorly documented; to the point that you can't even prove it is yours. It is completely uninsured, unaudited and untracked; you don't know what it's worth, or where it is. Your whole corporate culture accepts this state of affairs as its normal business practice.

Then you realize it's not a nightmare, it's true.

Your company's major asset is its confidential and proprietary information, its trade secrets, the knowledge required to run your business every day. More important and more valuable than all the buildings, machines and vehicles, it is irreplaceable. It is the one thing that differentiates you from your competitors and makes you successful.

And the odds are good that it is being stolen as you read this.

The Problem

Trade secrets are rapidly becoming the intellectual property of choice due to their advantages in the information economy. Machinery and mechanisms were the brainchildren of the Industrial

continued on page 7

SECURITIES

Warming Up to Stock Selling Plans: Upholding Rule 10b5-1's Affirmative Defense

By Sean T. Prosser

Maybe it was the declining stock market or maybe the rule was just too new, but many public companies initially were reluctant to encourage their executives to adopt written stock selling plans designed to comport with the defense against insider trading liability created by the new SEC Rule 10b5-1, 17 CFR 240.10b5-1.

To be sure, some executives quickly implemented selling plans, but many others remained hesitant to do so. In fact, some actually rescinded their brand-new plans in the face of declining stock prices and shareholder criticism. Clearly the falling market substantially dampened the initial appeal of such plans. Why would executives want to lock themselves into a selling strategy when prices are so low? Maybe it is a signal of the market turning,, or maybe the passage of time has alleviated concerns, but the number of companies amending their corporate insider trading policies to allow for such plans now is on the rise.

What Is the New Rule?

The affirmative defense against insider trading liability is just a subsection of the new Rule 10b5-1. See Rule 10b5-1(c). Primarily, the rule was the SEC's retort to several court decisions that had held that an insider trading claim is not stated unless it is demonstrated that the defendant actually used nonpublic material information when he or she made an investment decision, rather than the more lenient standard favored by the SEC requiring mere possession of the information. Rule 10b5-1 reflects the SEC's long-held position that insider trading liability arises when a person trades while only "aware" of material nonpublic information. See Rule 10b5-1(b).

Rule 10b5-1 adopts a general rule that any purchase or sale of stock while "aware" of material nonpublic information is illegal, without any need to show that the information was a motivating factor in making the trading decision. See Rule 10b5-1(b). In other words, the rule abolishes any distinction between "use" and "possession" of inside information and increases the risks for executives who sell stock, whatever the reason, at a time when they arguably know material undisclosed information.

continued on page 2

In This Issue

Trade Secrets

continued from page 1

Age, and patent law was designed to protect them. In the Information Age, trade secret protection is better suited to the fast-moving and unpatentable confidential information we need to run our companies. But companies have not yet developed an effective system for realizing the full value of trade secret rights.

The financial risks of loss are large. The Brookings Institution estimates that "at least 50 percent, and possibly as much as 85 percent" of the value of American companies is attributable to intangible assets.[1] This helps explain the large differences between book value and stock market capitalization. The difference represents the valuation the market has placed on intangible assets. If even half of the total market value is attributable to intangible assets, then the value of intangible assets for all publicly held companies in the United States would exceed $6 trillion. And, like tangible assets, directors and officers have a fiduciary obligation to protect these intangible assets.

At the same time that the information economy has made trade secrets more important, it has made them more likely to be stolen. A more mobile work force, increased use of contractors and consultants and increased outsourcing of infrastructure all provide opportunities for trade secret information to leave the company's control. Information technology itself contributes to the mobility of information.

Increasingly, information is stored in easily copied computer files, and Internet connectivity and high-density media such as CD-ROMs make these files easy to transport. A disgruntled employee can literally walk out the door with the company in his pocket.

But the risk of loss is much greater than just from disgruntled employees; any uninformed employee presents a risk. Today, many employees do not recognize that information to which they have access at work qualifies as trade secret information. Well-meaning employees routinely disclose trade secrets to trade show attendees, job candidates, the press and other third parties.

Without any systematic approach to the identification of trade secrets, it is often difficult to draw the line between an employee's general knowledge, skills and experience on the one hand, and the company's legitimate trade secret rights on the other. Many employees believe that they own all the work product of their efforts. This is a common point of view among technology professionals today.

The Law

The modern definition of trade secret encompasses any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.[2]

The law provides protection for trade secrets if certain legal requirements are met.[3] However, unlike patents, copyrights and trademarks, there is no office or agency where you can file a trade secret application, obtain a review by a qualified examiner and be issued an official trade secret certificate.

The legal protection of trade secrets instead requires self-administration by the trade secret owner. Traditionally, the intellectual property bar has recommended trade secret audits.[4] However, trade secret audits are expensive, and most companies do not spend the money to conduct them. Further, trade secret audits are only "snapshots" at a given point in time. The trade secret status of information assets is constantly changing and the results of trade secret audits can become quickly outdated.

At the present time, most companies wait until their trade secrets have been compromised, and then file suit for trade secret misappropriation. It is only then that trade secret rights are identified and protected. However, it is often too late to protect trade secrets at this stage. It is difficult, after the fact, to go back and prove the existence of a trade secret. Employees have retired or are deceased, memories have faded, documents no longer exist or cannot be found.

A trade secrets audit conducted during litigation is haphazard at best. Under the pressure of discovery deadlines, outside counsel scrambles to interview available witnesses and review mounds of documents to identify the trade secrets allegedly taken by the former employee. Under these circumstances, the company often loses the lawsuit. Identifying trade secrets after the fact often reveals a lack of reasonable measures to protect the trade secrets or any evidence that the employee even had access to them. Courts often take exception to imposing liability on a former employee for trade secret misappropriation when the company did not treat the information as a trade secret in the first instance.

And trade secrets, once lost, are lost forever.[5]

The Solution

Trade secrets require identification and protection. The starting point of any solution must therefore be an ongoing accounting system for trade secrets. A company must first know what they are and where they are located. The law has established a six-factor test for the identification of trade secrets that provides the benchmarks necessary for assisting a company in identifying trade secret assets.[6] These six factors are as follows:

Factor 1: The extent to which the information is known outside the company. The more extensively the information is known outside the company, the less likely it is a protectable trade secret.

Factor 2: The extent to which the information is known by

continued on page 8

R. Mark Halligan is a principal in the Chicago intellectual property firm of Welsh & Katz, Ltd. and a nationally recognized expert on trade secrets law (*www.rmarkhalligan.com*). **Richard F. Weyand** is president of The Trade Secret Office Inc. (*www.theTSO.com*). They are co-inventors of a patent-pending accounting system for the identification and protection of trade secrets called the Trade Secret Examiner.

Trade Secrets

continued from page 7

employees and others involved in the company. The greater the number of employees who know the information, the less likely it is a protectable trade secret.

Factor 3: The extent of measures taken by the company to guard the secrecy of the information. The greater the security measures, the more likely it is a protectable trade secret.

Factor 4: The value of the information to the company and its competitors. The greater the value of the information to the company and to its competitors, the more likely it is a protectable trade secret.

Factor 5: The amount of time, effort and money expended by the company in developing the information. The more time, effort and money expended by the company in developing the information, the more likely it is a protectable trade secret.

Factor 6: The ease or difficulty with which the information could be properly acquired or duplicated by others. The easier it is to duplicate the information, the less likely it is a protectable trade secret.

Applying these six factors, companies can identify trade secrets in advance of litigation, and then take the necessary steps to ensure that sufficient documentation is in place to identify these assets and that reasonable measures are in place to protect them.

This identification and protection of trade secrets is an ongoing and continuous process. An effective program requires the continuous classification of new trade secrets and the declassification of stale trade secrets that no longer have economic value.

Employee education must be an integral part of any trade secret protection plan. Employees must be made aware of their fiduciary duty to protect confidential information and periodically warned about situations that may result in the inadvertent loss of trade secrets. Processes must be in place for notifying employees of the company's trade secret rights and for protecting trade secrets as they are used in the company's business operations.

Finally, access to trade secret information must be tracked. Trade secrets should be disclosed internally only on a "need to know" basis. The emerging trend of posting confidential information on the company's internal web site—for all to see—is contrary to effective trade secret protection. The more people who have access to the information, the less likely the information will qualify as a trade secret.[7] Access to trade secret information should be strictly controlled, and access should be tracked so that the company can win the trade secret lawsuit against a former employee who denies knowledge of the trade secret in litigation.

The time has come to develop an effective accounting system for intangible trade secret assets. The identification and protection of trade secret assets can no longer be ignored until a trade secret misappropriation lawsuit is filed. Officers and directors have a fiduciary duty to identify these assets in the new economy; only then can these assets be effectively insured, valuated, licensed and protected. And only then will companies realize the full potential of the information economy and correct the current sorry state of trade secret protection.

---

(1) "New Ways Needed to Assess New Economy," Margaret Blair, Brookings Institution, Nonresident Senior Fellow, Economic Studies, in The Los Angeles Times, Nov. 13, 2000.

(2) See Restatement of the Law (Third) Unfair Competition § 39 (1995).

(3) The two primary requirements are (1) that the information not be generally known in the trade, and (2) that the trade secret holder take reasonable measures under the circumstances to protect the information as a trade secret. See generally, Uniform Trade Secrets Act, § 1(4) (definition of a "trade secret").

(4) See, e.g., R. Mark Halligan, Trade Secret Audits, *www.execpc.com/~mhallign/tradesec.html*

(5) *FMC Corp. v. Taiwan Tainan Giant Industrial Co.*, 750 F.2d 61, 63 (2d Cir. 1984).

(6) Restatement (First) of Torts § 757 (1939).

(7) "[T]he extent of a property right [in a trade secret] is determined by the extent to which the owner of the secret protects his interest from disclosure to others." *Ruckelhaus v. Monsanto*, 476 U.S. 986, 104 S.Ct. 2862 (1984).

Hotline

Recent Decisions Of Interest To the Corporate Counsel

ATTORNEY FEES

Rejection of Rule 68 Settlement Offer Limits Fees Plaintiff May Recover

The U.S. District Court for the Eastern District of Pennsylvania has ruled that a plaintiff in an employment discrimination suit is not entitled to attorney fees for work done after a formal pre-trial settlement offer is made, even if it is rejected by the plaintiff and followed by a jury award that is less than the defendant's offer. *Tai Van Le v. University of Pennsylvania*, No. CV. A. 99-1708 (July 13).

The plaintiff was an electronics engineer who filed suit against his employer claiming that he was fired for complaining about national origin harassment he received. At trial, a jury rejected his harassment claim but found the plaintiff had been the victim of retaliation and awarded him $25,000 in compensatory damages and $10,000 in punitive damages. Prior to trial, the plaintiff had rejected a settlement offer of $50,000 made pursuant to Rule 68 of the Federal Rules of Civil Procedure. Following the trial, the defense filed a post-trial motion seeking all costs it had incurred after making the settlement offer, as well as the attorney fees that were incurred in taking the case to trial. The plaintiff argued that the defense was not entitled to any fees or costs since the verdict, combined with the fees incurred up to the date of the offer, totaled more than $50,000.

The district court found that the plaintiff had to reimburse the defendant for any costs incurred after the formal offer was made, but that the defendant was not entitled to recover attorney fees for taking the case to trial. The court stated that while the U.S. Court of Appeals for the Third Circuit had never addressed this issue, several district courts within the circuit had, and they ruled that Rule 68 does not entitle the defense to any attorney fees. The

IP LAW360

Portfolio Media, Inc. | 648 Broadway, Suite 600 | New York, NY 10012
Phone: +1 212 537 6331 | Fax: +1 212 537 6371 | customerservice@portfoliomedia.com

Trade Secret Holding Companies: A Structural Solution To A Sarbanes-Oxley Requirement

--- It is now recognized that Sarbanes-Oxley requires corporate directors and officers to account for and manage the trade secret assets of public companies. The difficulties now center on implementation of these requirements. The creation of a holding company for trade secret assets provides a vehicle for complying with the SOX requirements and provides other benefits to the company.

Section 302 of Sarbanes-Oxley requires the CEO and CFO of public companies to certify that their annual and quarterly reports do not contain any untrue or misleading statements of material fact or material omissions. They must also certify that the financial information in the report fairly presents the financial condition of the company. As valuable assets that materially affect the financial condition of the company, trade secrets fall under Section 302.

In addition, Section 404 requires companies to document and certify the scope, adequacy and effectiveness of the internal control structure and procedures for financial reporting and controls, which should include internal controls and procedures for handling valuable trade secret assets. Finally, Section 906 imposes civil and criminal penalties for violations of Sarbanes-Oxley. Shareholder suits for non-compliance also loom on the horizon, and may well target officers and directors personally.

Yet trade secrets are among the most difficult assets of the company to quantify, or even to identify. The Seventh Circuit Court of Appeals recently noted that the existence of a trade secret is one of the most elusive and difficult concepts in the law to define. Faced with this challenge, U.S. corporations often ignore or sweep trade secret assets under the rug. They only surface, if at all, when a key employee leaves the company and a trade secret misappropriation lawsuit is filed. This state of affairs is no longer viable in view of the SOX requirements.

The existing atmosphere in most U.S. corporations is partially to blame for the sorry state of trade secret assets. The identification and protection of trade secret assets takes time, effort and money. Budgets are nonexistent or insufficient for these tasks. Too often trade secret protection is viewed as an administrative expense rather than an operational necessity. The result is that the company's trade secret assets are often left unprotected to the economic detriment of the company's shareholders.

* Importance of Trade Secrets *

Subtract your company's book value from its market capitalization, and in our modern information-oriented economy you will find that much of your company's value cannot be accounted for. Some of it is goodwill, branding, trademarks and patents, but the bulk of this unaccounted economic value is the company's trade secrets.

Trade secrets are differentiators. By definition, the company's trade secrets are comprised of information unknown to competitors that allows the company to derive competitive advantages in the marketplace. Trade secrets differentiate the company and its products from competitors, and therein lies their economic value. This economic value is perceived by the equity markets and reflected in the company's stock price

The law requires reasonable measures under the circumstances to protect trade secrets. Given the often enormous difference between the company's book value and actual marketplace capitalization, it should be apparent that trade secret assets must be identified and protected. Yet, today, many corporations do not document the existence and location of trade secret assets.

* Structural Bias *

One thing that places trade secrets at risk is the structural bias that account for what is easy rather than for what is important. The machine on the production floor, the fork lift, the computer you sit in front of and the desk it sits upon, the very chair you are sitting in—all have property tags. They are logged and tracked not because they are valuable, but because they are tangible. Yet there is no piece of furniture, no vehicle, no machine that is worth a fraction of your most valuable trade secret.

Even the question "What is your most valuable trade secret?" poses a conundrum. There is no trade secret control function within the corporation, no trade secret identification procedures, no trade secret classification procedures, and, of course, no trade secret valuations

Without a concrete asset to account for, U.S. companies have simply ignored trade secret assets. How many trade secrets does the company have? How much time, money and effort will be required to identify, classify and protect trade secret assets? Most U.S. corporations cannot answer these basic questions.

* A Trade Secret Holding Company *

The formation of a holding company for intangible assets has a lot of merit. In recent years, U.S. companies have begun to set up subsidiaries to license patent assets. Others advocate this approach for trademarks. Patents and trademarks are well defined by the application process, however, and thus easier to deal with by traditional methods. It is the inchoate mass of trade secret assets for which the holding company business model is particularly well suited.

In this model, the corporation sets up a wholly owned subsidiary for its trade secret assets and then transfers legal title to the company's entire portfolio of trade secrets assets to the newly established trade secret holding company. Under current IRS rules and regulations, this is not a taxable event. The corporation then enters into an exclusive license with the trade secret holding company to use the trade secret assets. This results in a number of business advantages.

First, the formation of a trade secret holding company with attendant reporting obligations to the parent can be easily tailored to comply with the Section 302 reporting and Section 404 process requirements under Sarbanes-Oxley with regard to trade secrets.

Second, a trade secret holding company need not be incorporated in the same state as the parent. By choosing a low-tax state for the trade secret holding company, the parent company can deduct the royalties as expenses in the high-tax state while enjoying tax savings on the royalty income received by the trade secret holding company in the low-tax state.

Third, the income earned from royalties by the trade secret holding company can be loaned back to the parent corporation. Interest on such loans will be treated as a business expense in the parent company's home state, resulting in an increase in net revenues to the parent corporation.

Fourth, the trade secret assets of the trade secret holding company, once accounted for, can now serve as collateral for loans or such assets can be licensed to third parties. Once again, the income from these activities can be loaned back to the parent company in the high-tax state, resulting in the same advantages outlined above.

Fifth, the income derived from the royalties and other income-producing activities of the trade secret holding company now provides the revenue source necessary to set up the dynamic systems required for the identification, classification, protection and valuation of trade secret assets.

* An Accounting System for Trade Secret Assets *

While all of the advantages discussed above are in themselves sufficient reason to pursue the business model of a trade secrets holding company, the greatest advantage may lie in the structural advantages that a trade secret holding company provides for the development and implementation of a trade secret accounting system.

The rules are well established for determining appropriate royalty rates for income-producing assets. There are also well-established rules for determining the costs of maintaining such assets. The existence of a trade secret holding company now provides the opportunity to apply these same principles to determine appropriate royalty rates and commensurate maintenance and accounting costs for trade secret assets.

As previously noted, the difference between the company's book value and its market capitalization defines the upper limit of the total value of the company's trade secret portfolio. Ratios can be developed to determine the respective values of brands, trademarks and other good will, and such ratios will vary from company to company. Applying these ratios, a reliable estimate of the total economic value of the trade secret portfolio can then be determined.

Based on the total value of the trade secret portfolio, appropriate royalty rates can be determined. Likewise, appropriate budgets for the maintenance and accounting of trade secret assets can be determined. The trade secret holding company's charter will be to maintain and account for these assets, and it will have the revenue stream necessary to both justify and finance these necessary operations for trade secret assets.

* A Profit Center, Not A Cost Center *

At this point it is appropriate to ask if a holding company merely adds another layer of bureaucracy to the task of identification, protection and valuation of trade secret assets. Does the trade secret holding company actually constitute a solution? Cannot these same tasks be handled by the parent company despite the advantages outlined above? Could these same processes be performed within the parent company?

Perhaps there is room for debate, but the record to date is clear. U.S. companies have a dismal track record when it comes to the protection, management and valuation of trade secret assets. Even well-intentioned efforts are short-lived when management attention moves on to other issues. Resources dissipate, budgets are cut, staff is laid off or reassigned under the twin pressures of staff and budget constraints. It is impossible in the U.S. corporate environment to develop long-term plans if trade secrets programs are considered a corporate "expense" and not a corporate "asset."

The trade secret holding company provides a structural solution and ensures compliance with the requirements of Sarbanes-Oxley because (1) it is a profit center, not a cost center, (2) it has a revenue stream, with both an obligation to protect that revenue stream and the resources to do so, (3) it results in a dedicated and experienced staff focused on trade secret assets that cannot easily be redirected to other projects in the parent corporation and (4) it reports through a direct line of communication with top management and the Board of Directors as required by Sarbanes-Oxley for this important asset class.

* Conclusion *

A wholly-owned subsidiary for trade secret assets provides the opportunity to solve longstanding problems relating to the proper management and accounting of trade secret assets. The establishment of a "trade secret holding company" will ensure compliance with the requirements of

Sarbanes-Oxley while at the same time providing other important financial benefits to U.S. corporations.

--By R. Mark Halligan and Richard F. Weyand

R. Mark Halligan is a Principal in the Chicago intellectual property law firm of Welsh & Katz Ltd. and focuses his practice on trade secret law. Richard F. Weyand is president of The Trade Secret Office Inc., which is developing methods and software for the automated discovery, inventory, evaluation and tracking of trade secret intellectual property assets.